Document Approval:

Issued by: R&D	Deepak Sharma		
	Name printed	Signature	Date
Approved by PL:	Deekha Banhoota		
	Name printed	Signature	Date
Approved by TEST:	Sravan K		
	Name printed	Signature	Date
Approved by QA:	Sreejith Viswam		
	Name printed	Signature	Date
Approved by R&D:	Sridhar Manickavel		
	Name printed	Signature	Date
Approved by Independent Reviewer:	Gerd Dautal		
	Name printed	Signature	Date

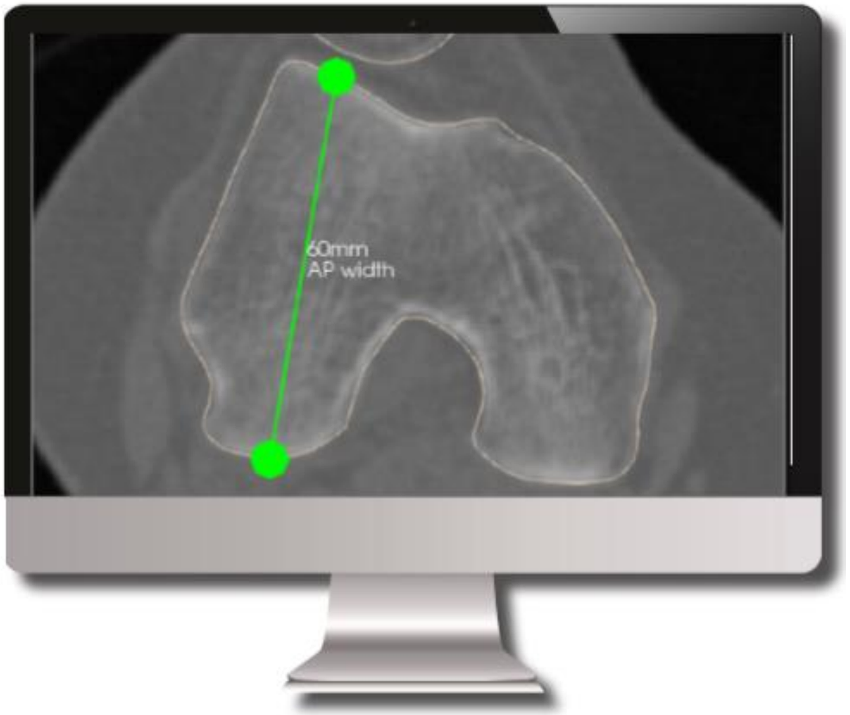
Security Operations Manual

D005010066

V 00

Formula 3D Knee navigation planning software

Security Operations Manual



Applies to 6007-670-000 V1.0

This document was prepared by **R&D** of **Stryker Global Technology Center** division. See section 3.1 below for contact information.

Table of Contents

1. PURPOSE

This Security Operations Manual (SOM) provides information that Stryker's customers need to know in order to integrate a specific Stryker device or health IT solution into a customer's IT network environment in a secured manner. It also supports a customer's ability to perform risk management, to identify configurable security controls, and to better protect their systems.

2. DEFINITIONS

API – Application Programming Interface: An interface for computing that defines interactions between multiple software intermediaries.

COTS – Commercial off-the-shelf: Software (or any other item) that is sold as a packaged solution which is then adapted to satisfy the needs of the organization purchasing the COTS. Some medical devices utilize COTS software in addition to or instead of software developed by the manufacturer. See third-party software.

Customer: The individual or organization responsible for procurement and operation of the device. See Owner and Operator.

Device: The item being integrated or used for a healthcare purpose. A Medical Device or other health IT product may be referred to as a Device or a Product in this document.

DICOM (Digital Imaging and Communications in Medicine): Standard developed by NEMA and the American College of Radiology, used worldwide to store, exchange, and transmit medical images.

FDA – U.S. Food and Drug Administration: A federal agency of the United States' Department of Health and Human Services. See www.fda.gov.

HDO – Healthcare Delivery Organization: Also "Health Delivery Organization," an organization or group of organizations that are involved with the delivery of healthcare services. A hospital is an HDO. If an HDO purchases and operates a Stryker device, the HDO is also the Customer, Owner, and Operator per the definitions of those terms.

IEC – International Electrotechnical Commission: A global organization whose work underpins quality infrastructure and international trade in electronic goods. IEC publishes thousands of international standards, including documents related to medical device software (e.g., IEC 62304). See www.iec.ch.

IFU – Instructions for Use: Information provided by the manufacturer in document or electronic form, informing the user of a device's intended purpose and proper use and of any precautions to be take.

ISO – International Organization for Standardization: An international standard-setting body that promotes proprietary, industrial, and commercial standards, and publishes standards relevant for information technology, privacy, and security (e.g., ISO/IEC 27034). See www.iso.org.

Manufacturer: The entity (Stryker) that builds the device and sells it to the customer.

MDR – European Union (EU) Medical Device Regulation of 2017: The European Union regulation concerning medical devices. See https://ec.europa.eu/health/md_sector/overview_en.

Medical Device: See the following sources if a precise definition is required: FDA, MDR (EU) 2017/745, ISO 14971:2007.

NEMA – National Electrical Manufacturers Association: See www.nema.org.

NIST - National Institute of Standards and Technology: A physical sciences laboratory and non-regulatory agency of the United States Department of Commerce. NIST has published comprehensive standards for the selection, implementation, and risk management of security and privacy controls (e.g., NIST SP 800-53). See www.nist.gov.

Operator: The person(s) using the device for its intended purpose. This term may also sometimes refer to the person or organization responsible for procuring the device (owner, customer).

OSS – Open Source Software: Third party software licensed under an OSS license, in which the copyright holder grants users the rights to use, study, change, and distribute the software to anyone and for any purpose as long as the license terms are adhered to.

Owner: See Operator and Customer.

PHI - Protected Health Information: Individually identifiable health information (IIHI) that is transmitted by electronic media; maintained in electronic media; or transmitted, or maintained, in any other form or medium (source: extracted from 45 CFR Section 160). Note: This is a subset of PII.

PII - Personally Identifiable Information: Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity… and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (source: from NIST SP 800-122).

Product: See Device.

SaMD - Software as a Medical Device: Software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device (source: from International Medical Device Regulators Forum).

SBoM – Software Bill of Materials: For a specific device, a listing of all software components that are incorporated into the final product. The SBOM may be used to assist with operational security planning by the HDO.

SOM - Security Operations Manual: A product-specific guide to the secure integration of a product into a customer IT network (this document).

Third-party software: Third party software is software not developed by Stryker, and for which Stryker otherwise does not have complete ownership. See COTS and OSS.

User: See Operator.

3. PRODUCT DESCRIPTION

Manufacturer Name	stryker
Stryker Division	Stryker Global Technology Center
Address	**Stryker Global Technology** **Center Private Limited** 10th Floor, Vatika Business Park, Block Two, Sector-49 ,Sohna Road, Gurgaon 122002, Haryana, India
Device Description	Formula 3D Knee navigation planning software is used to create a pre-operative planning for a knee replacement surgery where Stryker's Triathlon knee implant is used. The Formula 3D Knee navigation planning software is intended to provide a surgeon facing, easy to use CT Knee planning software, that uses the patient's CT scans to visualize the disease condition of Knee in three-dimension and enable effective decision making for the surgeons before they even go into the operating room on the day of the surgery.
Device Model, Version	**6007-670-000 V1.0** **(Further digits for minor fixes controlled internally)**
Manufacturer Contact Information	**Manufacturer:** **Stryker Global Technology Center Private Limited** 10th Floor, Vatika Business Park, Block Two, Sector-49 , Sohna Road, Gurgaon 122002, Haryana, India **Distributed By:** **Stryker Japan K.K.** 2-6-1, Koraku, Bunkyo-ku,Tokyo, 112-004, Japan t/f: 03-6894-0000 Additional information and contact links are available on Stryker's Product Security webpage, https://www.stryker.com/us/en/about/governance/cyber-security.html.

3.1 Device and Manufacturer Identification

Device :
Formula 3D Knee navigation planning software

Manufacturer:

Stryker Global Technology Center Private Limited
10th Floor, Vatika Business Park,
Block Two, Sector-49 ,Sohna Road,
Gurgaon 122002, Haryana, India

3.2 Device Intended Use

Formula 3D Knee Navigation Planning Software is indicated for pre-operative planning for a knee replacement surgery where Stryker's Triathlon knee implant is used. The Formula 3D Knee Navigation Planning Software is intended to provide a surgeon facing, easy to use CT Knee planning software, that uses the patient's CT scans to visualize the disease condition of Knee in three dimension and enable effective decision making for the surgeons before they even go into the operating room on the day of the surgery.

Functionality Includes:

- Auto-segmentation and landmark identification (manual modification possible)
- Effortless implant planning
- Saves the planned report for quick reference, The surgeon has the control and can choose how to interpret and use the results from the pre-operative planning.

Contraindication :

The surgeon needs to determine whether the patient's conditions are appropriate for this kind of procedure. The patients who have other type of metallic implants at or near the region of interest (Knee joint), which can create artefacts/noise on the CT Scan, are against the use of this system. In addition, some patients with advanced osteoporosis or deformities would be contraindicated like fused bone in the femur and tibia at the knee region.

3.3 Vulnerability Intake and Montoring

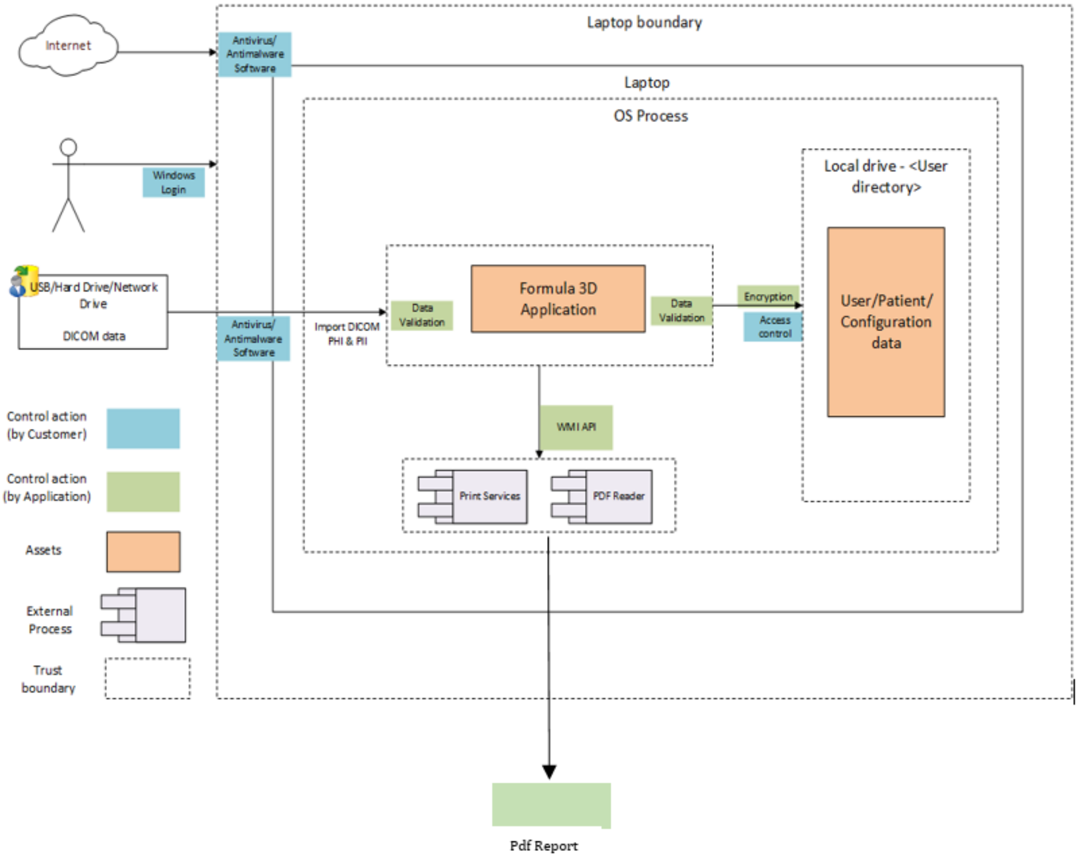
When Stryker obtains vulnerability information through surveillance or other sources, an assessment of the vulnerability's exploitability and impact is conducted. Based upon this assessment Stryker determines if further actions are required like providing security updates and/or providing communication to the customer in a timely manner. Vulnerability information may also be requested from Stryker at any time.

Any potential security vulnerabilities customer may become aware of due to Formula 3D Knee Navigation Planning Software shall be communicated to Stryker Customer Care and the same will be handled through the Post Market Complaint Management process to do the assessment and required actions including any updates needed for the customers.

3.4 System Characterization and System Assets

Formula 3D Knee Navigation Planning Software allow surgeon to create preoperative planning before proceeding to the surgery (Conventional or Navigated). This application allow to import/load Patients DICOM CT images from external storage devices such as USB, Hard disk and network drive. This application will not allow user to transfer the patient data to any other external or connected system to process futher. All the patient data is encrypted and stored locally under the logged user folder.

3.5 System Security Context and Intended Environment



While there is no specific requirement for Formula 3D Knee navigation planning software to be fully functional other than a usual windows environment, however Stryker recommends the user to follow some of the best practice security standards in order to run the application in a safe and secure environment as follows:

Devices operating in the intended use environment should consider that their IT infrastructure must obey different risk management approaches associated with their networks. HDO or Customer shall adopt a risk management process adhering to general cybersecurity best practices to maintain the healthcare provider's overall security status and their secure environment, as follows:

- Good physical security to prevent unauthorized physical access to Formula 3D Knee navigation planning software application.
- Access control measures (e.g., role based) to ensure only authenticated and authorized personnel are allowed access to network elements, stored information, services and applications.
- General patch management practices that ensure timely security patch updates.
- Malware protection to prevent unauthorized code execution.
- Security awareness training.

3.6 Setup of the SaMD (Software as a Medical Device) Formula 3D Knee navigation planning

The Formula 3D Knee Navigation Planning Software operates on Window-based PC

Operating system

Windows 10

CPU Intel Core i7-4770 or higher

RAM 32 GB memory or higher

Disk space

12 GB for program installation

500 GB or more for patient data storage

Monitor resolution 1920*1080 or above

Graphic board

Dedicated 4GB or higher memory (for example, Nvidia Quadro RTX3000 or NVIDIAT600)
Communication port USB 2.0 or higher

Optical mouse with left and right button, and scroll

Note:

• For cases where the patient data is loaded from local network drive, ensure network connectivity before starting the system. If there is a disruption in network connectivity, loading the data may take longer time than usual. If there is a disruption in network while loading the case, the software will notify the user.

• Information for compatibility with other devices. External hard drive to transfer CT data should be compatible with USB 2.0 or higher.

• For other Security related requirements please refer this manual.

4. MANAGEMENT OF PII and PHI

Formula 3D Knee Navigation Planning Software does not process PII/PHI oustide the surgeons laptop. The HDO has full control of its Laptop including the Formula 3D Knee Navigation Planning Software and responsibility for any PII/PHI there. The software will only display the PII/PHI information from the DICOM CT data or entered by the Surgeon and will not process it outside of the surgeon's laptop boundary. The HDO and User has the full control of the PHI and PII data in the Laptop and if any data to be removed based on the HDO data retention Policies, the HDO/ User can take support from Stryker to remove the data not needed to be retained.

4.1 Handling of Patient Requests for their PHI Access

Refer Section "Management of PII and PHI" above. User/ HDO has full control on patient data kept on laptop. Application do not have any additional functionality to provide access for patient requests. The HDO need to take the Report Output and share with Patients in cases where the Patient request his Personal Health Information as per the HDO process.

4.2 Storage and Removal of PII

Stryker does not process PII oustide the surgeons laptop. The HDO has full control of its Laptop including the Formula 3D Knee navigation planning software and responsibility for any PII there.

PII is embedded in the input DICOM files provided by the surgeon to the software. The software uses the PII data to display on its GUI and final planning pdf contains the PII information from DICOM files.

PII data will be maintained in volatile memory within the user laptop and can be exported to a pdf file. PII data is not transferred to any other system. User has the provision to anonymize the Patient Name on the Software GUI for the purpose of presenting the data for any external stake holders for training or other needs to support any privacy requriements for the HDO.

For backup and restore of PII data, please reach out to Stryker Customer care for support if needed.

5. AUTOMATIC LOGOFF

Customers are advised to configure windows OS to automatically lock the screen after a period of idle time as per the HDO IT policies.

Application also has the ability to lock the screen after inactivity for configurable timeout. User can configure the inactivity timeout. For details please refer User Manual Section **To configure System Settings.**

6. AUDIT CONTROLS

Stryker uses strong protection mechanism to protect the audit logs from getting tampered by any unauthorized party and hence does not require any extra steps from the users. Audit logs are encrypted using 256-bit AES encryption to avoid any tampering of the information. Decryption of the audit log is handled by Stryker on request from authorities. User cannot edit or alter the audit logs.

Formula 3D Knee Navigation Planning Software captures the following type of audit events:

- Creation/modification evets of patient PII data (No PII data stored)
- Import of DICOM data from removable media
- Application Programming Interface (API) and similar activity – Used for Printing and PDF view.
- Marked data with time stamp information to enable it to be selected for deletion based on when it was acquired or stored
-
- Work step visited, save / update operation on patient data.Application data - workflow and features executed.

Audit Logs Format is: {<timestamp>,<user>,<component>,<Feature/Module>,<Action>}

It is possible to export the logs via physical media considering the physical media like USB etc. to be secure. But it is recommended for the users to keep their physical media secure and updated against the latest threats.

Below are some of the safety measures that can be implemented to secure physical media like USB drive.

- **Do not plug a USB drive into an unknown computer.** Do not plug your USB into any computer without verifying the identity and safety of that computer system as the system may pose a potential security threat to your physical device.
- **Take advantage of security features.** Use passwords and encryption on your USB drive to protect your data, and make sure that you have the information backed up in case your drive is lost.
- **Disable Autorun.** The Autorun feature causes removable media such as CDs, DVDs, and USB drives to open automatically when they are inserted into a drive. By disabling Autorun, you can prevent malicious code on an infected USB drive from opening automatically.
- **Use and maintain security software and keep all software up to date.** Use a firewall, antivirus software, and anti-spyware software to make your computer less vulnerable to attacks, and keep the virus definitions current. Also, keep the software on your computer up to date by applying any necessary patches.

7. AUTHORIZATION

Formula 3D Knee navigation planning software requires a valid license in order to be fully functional and running., which needs to be obtained from Stryker only. Apart from requiring a valid license the application user shall leverage Windows Authentication and Autorization mechanism for User Access to Software and data. So, Stryker best recommends the user to setup proper authorization of users on their laptops as discussed below.

Authorization in system security is the process of giving the user permission to access a specific resource or function. In secure environments, authorization must always follow authentication. Users should first prove that their identities are genuine before an organization’s administrators grant them access to the requested resources. So proper authorization must be implemented at system level to harden the security. Different approaches to authorization may include:

- **Role-Based Access Control (RBAC):** Users are identified as being in a role that stipulates what privileges they have. Additionally, their user ID would restrict what data they have access to.
- **Access Control Lists (ACL):** An ACL specifies which users have access to particular resources. For instance, if a user wants to access a specific file or folder, their username or details should be mentioned in the ACL in order to be able to access certain data.

7.1 Access Prevention

Formula 3D Knee navigation planning software does not have any built-in access prevention features enabled in the Formula 3D Knee navigation planning software and leverages Windows Acceess Prevention mechanism. It is recommended to Customers to have proper access control measures as discussed in the below sections.

Taking steps to prevent unauthorized access to the system and its software components is important for a wide number of reasons, including preventing others from installing spyware and deleting your important files, or even creating viruses. By making changes to your computer to prevent unauthorized access, you are also protecting your personal privacy. Here are some steps to take to properly secure your computer and prevent others from accessing or modifying your application data:

- Set up password protection for user authentication: Password protection must be enabled at system level so that any unauthorized user cannot access the system. Password should be set in such a way that it must not be easy to guess. Also, strong password policy must be implemented to enhance the overall security of the system
- Install antivirus software or a spyware protection program: A good antivirus or spyware protection program must be installed on the system. These programs are used to detect any malicious actions or programs that might be used as a threat for the system or installed application. Lastly these antivirus programs must be regularly updated so that it can protect the system and the installed applications from latest security threats.
- Restrict the access to your system only to a limited number of trusted peoples. This can help the installed application to be accessed only by an authorized individual.

7.2 Privilege and Access

Stryker recommends the laptop Administrator to create separate users with appropriate privileges for access to Formula 3D Knee navigation planning software on the same laptop. Privilege and access to the Formula 3D Knee navigation planning software shall be restricted such that any user of the application can only use it within its intended use and any other functionality outside of the scope of the application is restricted as much as it can be. Users can maintain their own data on same laptop without access to other users data by setting different log in access.

8. CYBER SECURITY PRODUCT UPGRADES

The application does not have any updates installation policy implemented. Hence the users will not get any online updates. If any potential vulnarabilities are identified by Stryker which require an update at the customer site, a new version of the software will be released and customers will be informed about the action to be taken at their end.

It is HDO's responsibility to update the latest patches for their operating system, their third-party components (if any) and other applications like Virus Protection softwares/anti-malware softwares, Firewalls etc timely to ensure the security and protection of the system, Formula 3D Knee navigation planning software does not contain any malware protection embedded in itself.Hence, users are advise to install and anti-malware sofware on laptop.

9. HEALTH DATA DE-IDENTIFICATION

Formula 3D Knee navigation planning software anonymizes the data at runtime but does not delete or remove them. This can be done via GUI interface of the application itself.

Refer User Manual Section **Additional tools** for more details.

10. DATA BACKUP AND DISASTER RECOVERY

The application does not contain any online or offline mode of data backup or its recovery. So, the users are expected to have their own copy of data backup possibly in any physical media or via some online storage methods.

11. HEALTH DATA INTEGRITY AND AUTHENTICITY

No user actions are needed since any health data or other sensitive data stored on the system is encrypted using strong 256-bit AES encryption algorithm by the application itself to preserve the data integrity. The application properly checks the integrity of the data before loading them.

12. MALWARE DETECTION/PROTECTION

The standalone Formula 3D Knee navigation planning software by default does not contains any malware detection functionality and requires the user to have some malware detection in place. As, the Malware detection is crucial with malware's prevalence because it functions as an early warning system for the computer secure regarding malware and cyber-attacks. It keeps hackers out of the computer and prevents the information from getting compromised. This involves the process of scanning the computer and files to detect malware

To protect against the malwares below points are recommended:

- Install a good malware detection program on the system
- Keep your computer and software updated
- Use a non-administrator account whenever possible
- Think twice before clicking links or downloading anything
- Be careful about opening email attachments or images
- Don't trust pop-up windows that ask you to download software
- Limit your file-sharing

12.1 Other Compensation/Protection Controls

The Formula 3D Knee Navigation Planning Software application contains several protection mechanisms by its design like the application requires a valid license in order to work properly, the logs are encrypted using private keys and the data de-identification is also done which anonymizes the data at runtime. Besides these projections in place, Stryker recommend the users to apply certain other safety measure as below:

- The application should be allowed to be run only as authorized individual enabled using built in mechanism of windows OS.
- Proper Application whitelisting should be done on all security agents running on the device so that the Formula 3D Knee navigation planning software is not flagged as malicious in any case.
- Any third-party components installed in the system must be properly updated.
- Regular Antivirus scan should be done in order to eliminate any possible threats.
- Application Logs shall be audited for any errors or proper functioning of the application.
- Regular windows updates and patches should be installed.

12.2 Firewall Implementation

In order to safely use the application its important the below listed firewall rules be strictly followed and respected while using the application: -

- Ensure that you have enabled the firewall. If not, please follow the below steps on your Windows computer
  - Go to start and open Control Panel
  - Select **System and Security** > **Windows Defender Firewall**.
  - Choose **Turn Windows Firewall on or off**.
  - Select **Turn on Windows Firewall** for domain, private, and public network settings.

- Other things to consider: -
  - It is imperative that logs/warnings get the attention of the user any anomaly should then be resolved after its addressed.
  - Make sure that ports necessary for function are accessible only to authorized clients of the application.
  - In case a malware was reported on the system, ensure a proper sweep scan has been initiated and the removal of the malware was successful before resuming normal operations.

Firewall helps in preventing network access to devices. If properly used and configured it can lead to protected and reliable accessibility. It can help in prevention of unauthorized access and network connections against external threats, IP spoofing & routing attacks and malicious packets.

13. CONNECTIVITY CAPABILITIES

The Formula 3D Knee Navigation Planning Software application by default does not require any network connectivity or even wireless connectivity for its operation. The input CT data can be loaded from a network drive and the HDO IT to ensure adequate security controls to protect the network drive connected to the Laptop where Formula 3D Knee navigation planning software is installed. Also, it does not apply any restrictions in place when the physical media needs to be inserted in the system for data backup or data transmission.

So, it is advised for the users to use only secure and updated physical media in case it's required. To secure your USB or any physical media its best to properly scan them using a good antivirus program.

14. PERSON AUTHENTICATION

Formula 3D Knee navigation planning software does not provide any authentication mechanism apart from requiring a valid license which is unique for the system in order to be operational.

Stryker recommend the user to implement the secure windows authentication using strong password-based authentication on their latop. These password should be strong enough which is not easy to guess. Also, it must contain alphanumeric characters along with special characters to ensure best security practice.

For proper user management, the system should be configured for the below points.

- The authentication system should be done via password-based login or integrated windows-based authentication.
- After a few unsuccessful attempts account should lockout.
- Passwords must be changed after a regular interval of time.
- Default password or easy guess password must not be accepted by the system. In other words, the password should meet the password complexity policy.
- The system should be configured in such a way as to lockout itself if it's left idle after a reasonable period.
- Physical security should also be implemented to manage access to the system.

15. ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE

Stryker has evaluated Third Party components as per the requirement identified in IEC 62304 and adequate actions are implemented in application.

Stryker will be evaluating high risk third party components periodically and communicate to customers for any updates required during the Product lifecycle.

16. SYSTEM AND APPLICATION HARDENING

Stryker had performed the application security testing and security code review of Formula 3D Knee Navigation Planning Software. Formula 3D Knee Navigation Planning Software is hardened by eliminating any vulnerability or flaw which can lead to Security issue.

Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerability in the application, systems, and other areas. The goal of systems hardening is to reduce security risk by eliminating potential attack vectors and condensing the system's attack surface. By removing superfluous programs, accounts functions, applications, ports, permissions, access, etc. attackers and malware have fewer opportunities to gain a foothold within your IT ecosystem. Systems hardening demands a methodical approach to audit, identify, close, and control potential security vulnerabilities. The type of hardening you carry out depends on the risks in your existing technology, the resources you have available, and the priority for making fixes.

Stryker recommends to customers to keep below key points while implementing the system hardening.

- **Audit your existing systems:** Carry out a comprehensive audit of your existing technology. Use penetration testing, vulnerability scanning, configuration management, and other security auditing tools to find flaws in the system where the application is installed and prioritize fixes.
- **Create a strategy for systems hardening:** You do not need to harden all of your systems at once. Instead, create a strategy and plan based on risks identified within your technology ecosystem, and use a phased approach to remediate the biggest flaws.
- **Patch vulnerabilities immediately:** Ensure that you have an automated and comprehensive vulnerability identification and patching system in place.
- **Network hardening:** Ensure your firewall is properly configured and that all rules are regularly audited; secure remote access points and users; block any unused or unneeded open network ports; disable and remove unnecessary protocols and services; implement access lists; encrypt network traffic. Also refer to *Section 13*
- **Operating system hardening:** Apply OS updates, service packs, and patches automatically; remove unnecessary drivers, file sharing, libraries, software, services, and functionality; encrypt local storage; tighten registry and other systems permissions; log all activity, errors, and warnings; implement privileged user controls.
- **Eliminate unnecessary accounts and privileges:** Enforce least privilege by removing unnecessary accounts (such as orphaned accounts and unused accounts) and privileges throughout your IT infrastructure.
- **Anti-Malware installation:** The system running Formula 3D Knee navigation planning software should have proper Anti-Malware software installed with latest updates.

17. HEALTH DATA STORAGE CONFIDENTIALITY

The data at rest is encrypted using a strong encryption mechanism implemented within the application itself which safeguards the sensitive medical data from prying eyes.

18. TRANSMISSION CONFIDENTIALITY

Formula 3D Knee navigation planning software does not transmit the data over network or internet. End user inputs data into the software using removable media or from local system. The pdf output can be stored or exported on the removable media.

Below are some of the guidelines to the user to be followed while managing data confidentiality.

- **Manage data access**: Controlling confidentiality is, in large part, about controlling who has access to data. Ensuring that access is only authorized and granted to those who have a "need to know" goes a long way in limiting unnecessary exposure. Users should also authenticate their access with strong passwords and, where practical, two-factor authentication. Periodically review access lists and promptly revoke access when it is no longer necessary.
- **Physically secure devices**: Controlling access to data includes controlling access of all kinds, both digital and physical. Protect devices from misuse or theft by storing them in locked areas. Never leave devices or sensitive documents unattended in public locations.
- **Securely dispose of data**: When data is no longer necessary for any-related purposes, it must be disposed of appropriately.
- **Manage data acquisition:** When collecting sensitive data, be conscious of how much data is actually needed and carefully consider privacy and confidentiality in the acquisition process. Avoid acquiring sensitive data unless necessary; one of the best ways to reduce confidentiality risk is to reduce the amount of sensitive data being collected in the first place.
- **Manage data utilization:** Confidentiality risk can be further reduced by using sensitive data only as approved and as necessary. Misusing sensitive data violates the privacy and confidentiality of that data and of the individuals or groups the data represents.
- **Manage laptop**: Computer management is a broad topic that includes many essential security practices. By protecting devices, you can also protect the data they contain. Follow basic cybersecurity hygiene by using anti-virus software, routinely patching software, whitelisting applications, using device passcodes, suspending inactive sessions, enabling firewalls, and using whole-disk encryption.

19. SECURITY PROGRAM INTEGRATION

Formula 3D Knee navigation planning software is a standalone software installed on user laptop. The secure practices for the software are covered under Section 8 of this document.

Stryker has implemented incident response programs as part of complaint handling process for the product. The product is intended for Japan market only and user can call t/f: 03-6894-0000 to inform Stryker if any potential threat is identified in the software. Then, Stryker team will take the right steps to help the customer to deal with the situation.

Stryker has done extensive security testing of the Formula 3D Knee Navigation Planning Software application and implemented adequate actions to ensure protection from external threats. However, beyond this security measures in place, it is advised for the users to take a step ahead and follow some of the below guidelines to ensure better security postures.

- Do not plug any unknown physical media like USB etc. If it is required to plug in to the device, it must be scanned thoroughly using a strong anti-malware program.
- System should be scanned on a regular basis for any potential threats using Antimalware and/or Anti Virus softwares.

19.1 Risk Management

Stryker integrates cyber security risk management into its overall program for health and safety risk management. Both security and safety risk assessments were conducted for this device per guidelines in compliance with EN/ISO 14971 and Stryker Product Security procedures. Additionally, Stryker has a robust post-market security risk management process that monitors the ongoing security posture of this device and addresses any security incidents that might arise.

20. SECURE DECOMMISSIONING

Please reach out to Stryker customer care for secured decommissioning.